Multi-Factor Authentication (MFA) FAQ

Multi-Factor Authentication is here!
The U.S. Government, as part of its CyberSecurity National Action Plan, has mandated the use of Multi-Factor Authentication (MFA) for all federal government websites. In an effort to comply with these mandates and strengthen the security of our websites, GSA will implement MFA and new password policies on GSA Fleet Applications, GSA Advantage, GSA eBuy, and GSA Global Supply.

What is Multi-Factor Authentication?
Multi-factor Authentication (MFA) is a systems access authentication method in which a user is granted access only after successfully presenting **two** or more pieces of evidence (or factors) to an authentication mechanism. This extra layer of security protects you, your agency or organization, and the government by making it more difficult for someone to gain unauthorized access to your user account.

What will the new login process look like?
Every time you login to a GSA Fleet application, you will be required to enter your email address, password, and a one-time verification code. Please note that we will discontinue the use of the User ID login. Your email address will replace your User ID.

Will I be required to update my password?
As an added security feature, GSA has implemented policies requiring stronger passwords that meet National Institute of Standards of Technology (NIST) requirements. The first time you login after the implementation of MFA in any of the GSA Fleet applications, you can login using the TEMPORARY password sent to your email or you will have the ability to change your password to meet the new length and complexity requirements. Additionally, you will be required to change your password every 90 days. Keep in mind that these credentials (emails, password and security question / answer) are unique and are the only one's required to access your GSA Fleet applications.

What are the new steps for logging in?
1. Enter the email address and password associated with your account.
2. You will be prompted to receive a system-generated one time password (OTP) verification code via email.
3. Enter the verification code into the field labeled "Enter Code" and click the "Verify" button. *Note that the verification code is valid for only 5 minutes*.

What if I never received my one time validation code?
On the login page, click the "Re-Send email" to receive another OTP code. If you don't receive this code, please report this to the helpdesk (see Help Desk)

How many tries do I get to login before my account is locked out?
After 5 failed attempts your account is locked out. You will need to contact the Helpdesk.

How long is my account active?
Accounts are active for 90 days after your last login. If you haven't logged in for 80 days, you will receive an email warning you that your account will be deactivated if you do not login.

What if the email address associated with my account is wrong?
Please contact helpdesk, and they will work to get your account updated.

If you need assistance contact Help Desk!
Contact helpdesk for:

For GSA Fleet Drive-thru and Vehicle Fleet Exchange (VFE):
Email:gsadrivethruhelp@gsa.gov | Phone: 866-472-6711

For GSA Vehicle Dispatch & Reservation Module (DRM), Federal Motor Vehicle Registration System (FMVRS), FedFMS and FMS2Go :
Email:gsafleet@gsa.gov | Phone: 866-472-6711

For GSA Short Term Rental (STR), Auto Auctions, Auto Choice, Auto Vendor, GSA Fleet Automated Remarketing Module (ARM) and GSA Fleet2Go:
Email:FleetAlert@gsa.gov